Journal of Number Theory 131 (2011) 2282–2302

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Strong approximation in the Apollonian group

Elena Fuchs

Institute for Advanced Study, School of Mathematics, Einstein Drive, Princeton, NJ 08540, USA

ARTICLE INFO

Article history:
Received 13 September 2010
Revised 24 March 2011
Accepted 18 May 2011
Available online 6 August 2011
Communicated by Ronald Graham

Keywords:
Apollonian circle packings
Affine sieve
Congruence obstructions
Local to global

ABSTRACT

The Apollonian group is a finitely generated, infinite index subgroup of the orthogonal group $O_Q(\mathbb{Z})$ fixing the Descartes quadratic form Q. For nonzero $\mathbf{v} \in \mathbb{Z}^4$ satisfying $Q(\mathbf{v}) = 0$, the orbits $\mathscr{P}_{\mathbf{v}} = A\mathbf{v}$ correspond to Apollonian circle packings in which every circle has integer curvature. In this paper, we specify the reduction of primitive orbits $\mathscr{P}_{\mathbf{v}}$ mod any integer $d > 1$. We show that this reduction has a multiplicative structure, and that mod primes $p \geqslant 5$ it is the full cone of integer solutions to $Q(\mathbf{v}) \equiv 0$ for $\mathbf{v} \not\equiv \mathbf{0}$. This analysis is an essential ingredient in applications of the affine linear sieve as developed by Bourgain, Gamburd and Sarnak.

1. Introduction

An Apollonian circle packing (ACP) is constructed by repeatedly inscribing circles into the triangular interstices in a Descartes configuration of mutually tangent circles or lines. Fig. 1 depicts the construction of two types of ACP's, bounded and unbounded: both start with four mutually tangent circles (in the unbounded case, two of the circles are parallel lines which can be considered to be tangent at infinity), and, continued indefinitely, yield packings of infinitely many circles. The unbounded packing constructed in the second picture of Fig. 1 is in fact the only kind of unbounded packing considered in this paper.

ACP's date back to Apollonius of Perga, who was interested in them in the context of compass and straight edge constructions of mutually tangent circles and lines. His theorem below ensures that the construction of ACP's described above is well defined, since it implies that there is precisely one circle one can inscribe in each triangular interstice in Fig. 1.

Theorem 1.1 *(Apollonius, circa 200 BC). To any three mutually tangent circles or lines there are precisely two other circles or lines which are tangent to all three.*

E-mail address: efuchs@math.ias.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2011.05.010

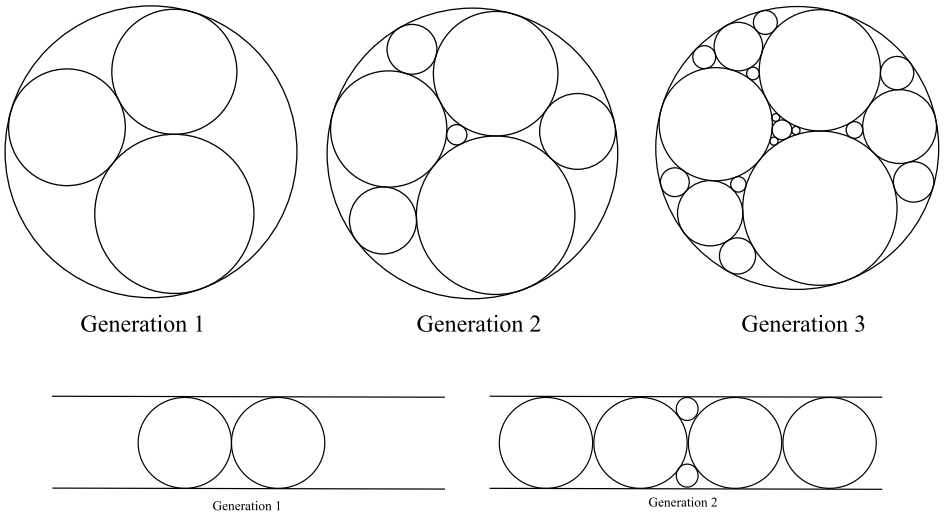

Fig. 1. Constructing an Apollonian circle packing: bounded and unbounded.

The study of ACP's has seen many facets of mathematics since. In this paper, we focus on number-theoretic aspects of *integral* ACP's which were noticed first by Frederick Soddy in 1936, who discovered that if any four mutually tangent circles in a bounded ACP have integer curvature,[1] all of the circles in the packing will have integer curvature as well. For example, the packing in Fig. 2 is generated by starting with circles of curvatures 1, 2, 2, and 3, and so consists of circles of integer curvature only. This packing immediately gives rise to infinitely many other integer ACP's simply by scaling all of the curvatures in the packing by an integer. However, it is more interesting to consider integer packings which do not arise from such a scaling process – i.e. packings in which the curvatures do not all share a factor > 1. Such packings are called *primitive* and there are in fact infinitely many bounded primitive integral ACP's. However, the only unbounded primitive integral packing is generated by starting with circles of curvatures 0, 0, 1, and 1 as in Fig. 3 (see [11] for a discussion).

Soddy deduced the integrality property of ACP's from the following theorem of Descartes (more recently re-proven by Coxeter in [4]) which he generalized to higher dimensions in a poem in [19].

Theorem 1.2 *(Descartes, 1643). If a, b, c, and d denote the curvatures of four pairwise externally tangent circles with distinct tangency points, then*

$$Q(a,b,c,d) = 2\left(a^2+b^2+c^2+d^2\right) - (a+b+c+d)^2 = 0. \tag{1.1}$$

Note that while Descartes' theorem originally applies to externally tangent circles only, it holds for a quadruple of tangent circles where one is internally tangent to the other three as in Fig. 1 if one takes the external circle to have negative curvature (see [12] for an explanation of this).

A solution (a,b,c,d) to Eq. (1.1) is called a *Descartes quadruple*, and the form Q is known as the *Descartes quadratic form*. It is at the core of what is known with regards to the number theory pertinent to integral ACP's. In 1943, Hirst derived from Theorem 1.2 that the curvatures in an ACP correspond to coordinates of vectors in orbits of a subgroup $A \subset \mathrm{O}_Q(\mathbb{Z})$ in the cone $Q(\mathbf{v}) = 0$, where $\mathrm{O}_Q(\mathbb{Z})$ denotes the orthogonal group preserving Q (see [13]). Combined with Soddy's observation, Hirst's discovery implies that the study of curvatures in integral ACP's is in fact a study of integral orbits of this group, which is appropriately called the Apollonian group.

[1] By curvature we mean reciprocal of the radius.

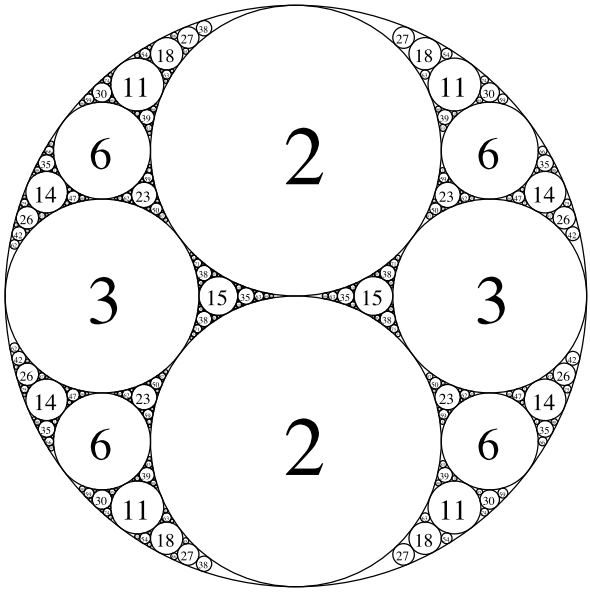

Fig. 2. Apollonian circle packing $(-1, 2, 2, 3)$.

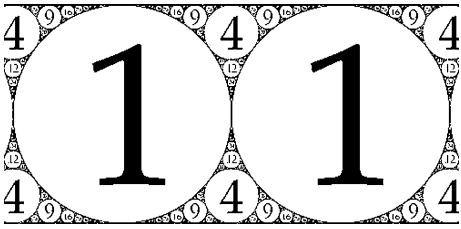

Fig. 3. Apollonian circle packing $(0, 0, 1, 1)$.

There are several fundamental questions to consider in the case of integral ACP's which were first formulated and addressed by the five authors Graham, Lagarias, Mallows, Wilks and Yan in [11]. They outline several important problems regarding integral ACP's, many of which have now been solved in [1,8,9,15].

One problem Graham et al. consider is that of determining congruence obstructions for curvatures in integral ACP's. Note that this question is most interesting in the case of primitive integral ACP's: otherwise there are obvious congruence obstructions modulo the gcd of all the curvatures.

Using the fact that A has several unipotent subgroups, they are able to show:

Theorem 1.3 *(Graham, Lagarias, Mallows, Wilkes, Yan, 2003). Let P be a primitive integral Apollonian circle packing. For any integer m with $\gcd(m, 30) = 1$, every residue class mod m occurs as the value of a curvature of some circle in the packing P.*

Upon collecting data for several ACP's, they also conjecture that there should be some congruence conditions mod 12 or 24 which completely determine all *large* integers appearing as curvatures in a primitive ACP. In this paper, we give a complete description of the reduction of the Apollonian group mod integers $d > 1$, which in turn yields a description of the collection of curvatures in any primitive ACP mod d. As a consequence of this description, we are able to fine-tune Theorem 1.3 by replacing 30 with 6 in Corollary 4.5, which we show cannot be improved further. In addition, our

analysis of the orbit mod powers of primes clarifies why the only congruence obstructions for integral ACP's appear to be modulo 24 – this was previously seen only through numerical experiments (for a detailed discussion of this, see [9] as well as Conjecture 1.5).

Our method is to consider the preimage Γ of A in the spin double cover of SO_Q. We determine Γ explicitly in Section 2, and rely on Dickson's classification of subgroups of SL_2 over finite fields (see [14]) combined with Goursat's lemma (see Theorem 2.6) to specify the mod d structure of Γ for square-free d. We extend this to powers of primes and non-square-free d in Section 3, and then use this to determine the precise mod d structure of any orbit $\mathscr{P}$ of A in Section 4. Our main result is stated in the following theorem.

Theorem 1.4. *Let $\mathscr{P}$ be an orbit of A acting on a Descartes quadruple $\mathbf{v}_P \in \mathbb{Z}^4$ of curvatures in a primitive packing P and let $\mathscr{P}_d$ be the reduction of this orbit mod an integer $d > 1$. Let $C = \{\mathbf{v} \neq \mathbf{0} \mid Q(\mathbf{v}) = 0\}$ denote the cone without the origin, and denote by C_{p^r} the cone mod p^r as defined in* (4.2)*. Write $d = d_1 d_2$ with $(d_2, 6) = 1$ and $d_1 = 2^n 3^m$ where $n, m \geqslant 0$.*

(i) *If $d_1 \neq 1$, the natural projection $\mathscr{P}_d \longrightarrow \mathscr{P}_{d_1} \times \mathscr{P}_{d_2}$ is surjective.*
(ii) *The natural projection $\mathscr{P}_{d_2} \longrightarrow \prod_{p^r \| d_2} \mathscr{P}_{p^r}$ is surjective and $\mathscr{P}_{p^r} = C_{p^r}$.*
(iii) *If $m, n \geqslant 1$, the natural projection $\mathscr{P}_{d_1} \longrightarrow \mathscr{P}_{2^n} \times \mathscr{P}_{3^m}$ is surjective.*
(iv) *If $n \geqslant 4$, let $\pi : C_{2^n} \longrightarrow C_8$ be the natural projection. Then $\mathscr{P}_{2^n} = \pi^{-1}(\mathscr{P}_8)$.*
(v) *If $m \geqslant 2$, let $\phi : C_{3^m} \longrightarrow C_3$ be the natural projection. Then $\mathscr{P}_{3^m} = \phi^{-1}(\mathscr{P}_3)$.*

Theorem 1.4 is a crucial ingredient in applications of the recently developed affine sieve of Bourgain, Gamburd and Sarnak (see [2]) in the context of integer ACP's. For example, it is used in [9] to give a precise asymptotic (conditional on randomness of the Möbius function) for the number of circles of prime curvature less than X. Another application of the affine sieve is proving the finiteness of the *saturation number* for certain integer-valued polynomials on orbits of various groups. In the case of the Apollonian group A, Bourgain et al. prove in particular that, given a polynomial f in four variables which is integer-valued and primitive[2] on a given integer orbit $\mathscr{P}$ of A, there is a positive integer r_0 such that for any $r \geqslant r_0$ the points $\mathbf{x} \in \mathscr{P}$ for which $f(\mathbf{x})$ has at most r prime factors in Zariski dense in the Zariski closure of $\mathscr{P}$. Theorem 1.4 would be necessary in using the affine sieve to determine this r_0 explicitly. However, one would need in addition a nontrivial lower bound on the gap between the first two eigenvalues of the Laplacian of $A\backslash\mathbb{H}^3$ which is still unknown. For this reason, it is difficult to prove good lower bounds for r_0 in the Apollonian case, as in many other problems of this type.

Even with these difficulties, because the Apollonian group is thin in the sense that it is of infinite index in the integer points of the orthogonal group fixing Q, the affine sieve is currently the most effective tool in tackling Diophantine problems such as counting circles of prime or almost prime[3] curvature – in particular, classical methods such as the theory of automorphic forms do not apply here. One can think of Theorem 1.4 as an analog of the Chinese remainder theorem which is a key ingredient in applying the affine sieve to orbits of the Apollonian group. In fact, Theorem 1.4 is a stronger result than needed for the sieve, since it specifies the structure of the orbit mod integers which are not square-free (the sieve only needs information about the square-free case). Essentially, it tells us that once we determine the structure of an orbit of A mod 3 and 8, we can deduce its structure mod d for any integer $d > 1$ from the well-understood local structure of the cone C above. Since there are only two possible orbits of A mod 3 and less than 300 orbits of A mod 8, Theorem 1.4 gives an effective way of determining the structure of any primitive ACP mod d, and is the key observation behind the local to global principle for ACP's as conjectured in [9]:

[2] We say that the polynomial is primitive on the orbit if for every $q \geqslant 2$ we have at least one point $\mathbf{x}$ in the orbit for which $(f(\mathbf{x}), q) = 1$.
[3] Almost primes are integers with few prime factors.

Conjecture 1.5 *(Fuchs, Sanden, 2010). Let P be an integral ACP and let P_{24} be the set of residue classes mod 24 of curvatures in P. Then there exists $X_P \in \mathbb{Z}$ such that any integer $x > X_P$ whose residue mod 24 lies in P_{24} is in fact a curvature of a circle in P.*

Proving such a rich local to global principle in the case of an orbit of a thin group is very difficult at this time. One might convince oneself that Conjecture 1.5 is true by considering an analogous problem that all large integers satisfying certain local conditions should be represented by a general ternary quadratic form – namely, we fix one of the curvatures in Descartes' form and solve the problem for the resulting ternary form. While the general case of this problem is resolved in [3] and [6], the results there are not effective and further work would be needed to obtain a precise result such as the one implied in Conjecture 1.5.

1.1. The Apollonian group

Recall from Theorem 1.2 that if a, b, c, and d are curvatures of four mutually tangent circles with distinct tangency points,

$$Q(a,b,c,d) = 2\left(a^2+b^2+c^2+d^2\right) - (a+b+c+d)^2 = 0$$

and that in the context of ACP's the outside circle in a bounded packing (which is internally tangent to the other circles) must have negative curvature to satisfy the equation. Note that fixing three of the curvatures (say b, c, d) above yields a quadratic equation which has two solutions $a = a_+, a_-$ such that

$$a_+ + a_- = 2(b+c+d).$$

In fact, the circles C_{a_+} and C_{a_-} of curvatures a_+ and a_-, respectively, are precisely the only two circles tangent to all three of the mutually tangent circles of curvature b, c, and d as stated in Theorem 1.1. In fact, one can solve for all of the curvatures in a given packing P by continuously fixing three known curvatures of mutually tangent circles and solving (1.1) for the fourth. In this way, one can deduce (see [12]) that if $\mathbf{v} = (a,b,c,d)^{\mathrm{T}}$ is a vector of curvatures of mutually tangent circles in a packing P, all of the curvatures of circles in P are given by the coordinates of vectors in the orbit $A\mathbf{v}$, where A is a group generated by

$$S_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$
$$S_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad S_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix}. \tag{1.2}$$

Since the orbits of A acting on Descartes quadruples are in one-to-one correspondence with Apollonian circle packings, A is known as the Apollonian group. Note that $S_i^2 = I$ for $1 \leqslant i \leqslant 4$, and there are in fact no other relations among the generators of A (see [12] for a discussion of the relations among S_i as well as the correspondence of ACP's to orbits of A).

Throughout this paper, the Apollonian group will be our main tool in analyzing ACP's, and we list some of its properties in the following lemma:

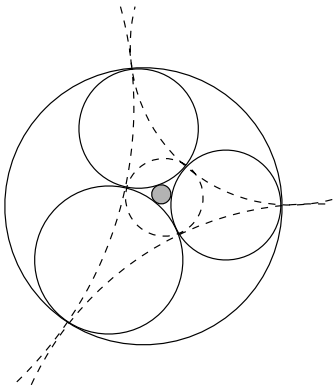

Fig. 4. Dual circles in an Apollonian circle packing.

Lemma 1.6. *Let A be the Apollonian group and let Q be the Descartes quadratic form. Then*

(i) *A is an infinite-index subgroup of the orthogonal group $\mathrm{O}_Q(\mathbb{Z})$ fixing Q,*
(ii) *A is Zariski dense in $\mathrm{O}_Q(\mathbb{C})$.*

Before proving Lemma 1.6, it is useful to consider the geometric representation of the generators of A. Note that Q has signature $(3,1)$, and so A can be regarded as a subgroup of $\mathrm{O}_{\mathbb{R}}(3,1)$, the isometry group of hyperbolic space $\mathbb{H}^3$. Its action on $\mathbb{H}^3$, as well as its action on a given quadruple of mutually tangent circles in a packing, can be realized by considering the upper half-space model of

$$\mathbb{H}^3 = \left\{(x, y, z) \in \mathbb{R}^3 \;\middle|\; z > 0\right\}$$

and embedding a Descartes quadruple of circles (C_1, C_2, C_3, C_4) (for example, the four largest circles in the packing, or those in generation 1) in the complex plane bounding $\mathbb{H}^3$. For any triple of mutually tangent circles (C_1, C_2, C_3) there is a unique *dual circle* or line $\mathscr{D}_{123}$ which passes through the tangency points of the three. The generators S_1, S_2, S_3, S_4 of A in (4.9) are then precisely reflections in $\mathscr{D}_{234}$, $\mathscr{D}_{134}$, $\mathscr{D}_{124}$, $\mathscr{D}_{123}$, respectively. Four such dual circles are drawn in dotted lines for the circle packing in Fig. 4. The shaded circle on the inside is the image of the outside circle under reflection through the smallest of the dual circles. The action of A on $\mathbb{H}^3$ is then realized as reflections through the hemispheres lying above the dual circles (which are also embedded in $\mathbb{C}$) of the packing, and a fundamental domain for this action is the union of the exteriors of the hemispheres lying above $\mathscr{D}_{234}$, $\mathscr{D}_{134}$, $\mathscr{D}_{124}$, $\mathscr{D}_{123}$, the dual circles corresponding to the largest four mutually tangent circles in the packing (see Section 2.2 of [15] for a detailed discussion of the action of A on $\mathbb{H}^3$).

This fundamental domain clearly has infinite volume, and so A is an infinite-index subgroup of the orthogonal group $\mathrm{O}_Q(\mathbb{Z})$ as stated in part (i) of Lemma 1.6. In this sense, the Apollonian group is a thin group, and this makes integral ACP's virtually unapproachable via classical methods such as the theory of automorphic forms. However, the richness of the group implied by part (ii) of the lemma is precisely the necessary condition for the analysis in [2] and [20] to apply in this case. We prove part (ii) below.

Proof of Lemma 1.6(ii). The Zariski closure G of the Apollonian group A is an algebraic group defined over $\mathbb{R}$, where $G(\mathbb{R})$ is a Lie subgroup of $\mathrm{SL}_2(\mathbb{C})$. Therefore G could be either the full orthogonal group or one of the following:

- A finite group: since A itself is not finite (for example, the unipotent element S_1S_2 has infinite order), its closure cannot be finite.

- The group SO_Q: since the generators of A all have determinant -1, this cannot be the closure of A.
- A torus or parabolic subgroup: it is known (see [17], for example) that the Hausdorff dimension of the limit set of A is $\delta = 1.3056\ldots$. If G were a torus or parabolic, we would have $\delta = 0$, giving a contradiction.
- The orthogonal group fixing the ternary quadratic form Q' of signature $(2,1)$ over $\mathbb{R}$ obtained by fixing one of the variables in (1.1). If this were the case, then we would have $\delta = 1$, again giving a contradiction to $\delta = 1.3056\ldots$.

Since the Zariski closure of A is none of the above groups, it must be the full orthogonal group, and so A is Zariski dense in $\mathrm{O}_Q(\mathbb{C})$. □

It is precisely the fact that A is Zariski dense in $\mathrm{O}_Q(\mathbb{C})$ that makes its orbits manageable via the affine sieve described in [2] even though it is a thin group. We rely heavily on this fact in what follows.

2. Congruence obstructions: the square-free case

In this section we determine the reduction of any integer orbit $A\mathbf{v}$ of the Apollonian group mod square-free integers $d > 1$ in order to establish the analog of the Chinese remainder theorem over the integers in the context of the group itself. A theorem of Weisfeiler (see Theorem 2.1) implies that a strong approximation principle should exist for the Apollonian group given Lemma 1.6 and we fine-tune this theorem in our case to specify the precise congruence obstructions in this section.

Note that it is convenient to work with the preimage of A in the spin double cover of SO_Q rather than the Apollonian group itself. The main reason for this is that A is a subgroup of the orthogonal group $\mathrm{O}_{\mathbb{R}}(3,1)$ where strong approximation does not hold, and it is difficult to say anything about the projection of A into $\mathrm{O}_Q(\mathbb{Z}/p\mathbb{Z})$ by working in the orthogonal group alone. However, the preimage Γ of A under the *spin homomorphism* in (2.1) is a Zariski dense subgroup of $\mathrm{SL}_2(\mathbb{C})$ where general results regarding strong approximation are known. Specifically, Weisfeiler proves the following in [20]:

Theorem 2.1 *(Weisfeiler, 1984). Let $\mathcal{O}$ be the ring of integers of a number field k, let V be the set of non-archimedean non-equivalent valuations of k, and let k_v denote the completion of k at a valuation $v \in V$. Let G be an absolutely almost simple, simply connected algebraic group over k, and let $\Gamma \subset G(\mathcal{O})$ be a Zariski dense subgroup of G so that the subfield of k generated by* 1 *and the traces of $\mathrm{Ad}\,\Gamma$ is k itself. Then there exists a finite subset $S \subset V$ such that the closure of Γ in $G(\prod_{v\notin S} k_v)$ is open.*

In the context of the Apollonian group, the field k in Theorem 2.1 is $\mathbb{Q}(\sqrt{-1})$, the ring of integers $\mathcal{O} = \mathbb{Z}(\sqrt{-1})$, and Γ is a Zariski dense subgroup of $G = \mathrm{SL}_2(k')$ where $k' = \mathbb{C}$ is the algebraic closure of k. For this case Weisfeiler's theorem implies that there is a finite set of primes $\mathfrak{P}$ in $\mathcal{O}$, so that Γ projects onto $\mathrm{SL}_2(\mathbb{Z}(\sqrt{-1})/\mathfrak{p})$ for $\mathfrak{p} \notin \mathfrak{P}$. However, Theorem 2.1 does not specify what $\mathfrak{P}$ is, and its proof does not easily imply what this set should be. It also does not give the multiplicative structure present in Theorem 1.4. In what follows we determine $\mathfrak{P}$ for our case and apply it in the context of orbits of A.

2.1. The preimage Γ of A in $\mathrm{SL}_2(\mathbb{C})$

Since strong approximation does not hold in $\mathrm{O}_Q(\mathbb{Z})$, we consider the mod $\mathfrak{p}$ reduction of the preimage Γ of $A \cap \mathrm{SO}_Q(\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{C})$ under the spin homomorphism ρ. As strong approximation does hold in SL_2, it is the natural setting in which to ask this question – we then map back to A via the spin homomorphism in order to complete the analysis of the orbits.

We recall from [7] that there is a two-to-one homomorphism ρ defined over $\mathbb{Q}$ from $\mathrm{SL}_2(\mathbb{C})$ into the special orthogonal group SO fixing the Lorentzian quadratic form $\tilde{Q}(x_1, x_2, x_3, x_4) = x_1^2 - x_2^2 - x_3^2 - x_4^2$:

$$\mathrm{SL}_2 \xrightarrow{\rho} \mathrm{SO}_{\tilde{Q}}. \tag{2.1}$$

The homomorphism ρ is defined explicitly in [7] for M in $\mathrm{SL}_2(\mathbb{C})$: For

$$M = \begin{pmatrix} a_0 + a_1\sqrt{-1} & b_0 + b_1\sqrt{-1} \\ c_0 + c_1\sqrt{-1} & d_0 + d_1\sqrt{-1} \end{pmatrix}, \tag{2.2}$$

we have[4] that $\rho(M)$ is

$$\begin{pmatrix} \frac{a_0^2+b_0^2+c_0^2+d_0^2+a_1^2+b_1^2+c_1^2+d_1^2}{2} & \frac{-a_0^2+b_0^2-c_0^2+d_0^2-a_1^2+b_1^2-c_1^2+d_1^2}{2} & -a_0b_0 - d_0c_0 - a_1b_1 - c_1d_1 & -a_0b_1 + d_0c_1 + a_1b_0 - d_1c_0 \\ \frac{-a_0^2-b_0^2+c_0^2+d_0^2-a_1^2-b_1^2+c_1^2+d_1^2}{2} & \frac{a_0^2-b_0^2-c_0^2+d_0^2+a_1^2-b_1^2-c_1^2+d_1^2}{2} & a_0b_0 - d_0c_0 + a_1b_1 - c_1d_1 & a_0b_1 + d_0c_1 - a_1b_0 - d_1c_0 \\ -a_0c_0 - d_0b_0 - a_1c_1 - b_1d_1 & a_0c_0 - d_0b_0 + a_1c_1 - b_1d_1 & a_0d_0 + c_0b_0 + b_1c_1 + a_1d_1 & a_0d_1 - d_0a_1 - c_1b_0 + b_1c_0 \\ a_0c_1 - d_0b_1 - a_1c_0 + b_0d_1 & -a_0c_1 - d_0b_1 + a_1c_0 + b_0d_1 & -a_0d_1 + a_1d_0 - b_0c_1 + b_1c_0 & a_0d_0 - b_0c_0 + a_1d_1 - b_1c_1 \end{pmatrix}.$$

In order to determine the preimage of $A \cap \mathrm{SO}_Q$, we relate the Descartes form to $\tilde{Q}$ as follows.

Lemma 2.2. *Let Q be the Descartes quadratic form as before, and let*

$$\tilde{Q}(x_1, x_2, x_3, x_4) = x_1^2 - x_2^2 - x_3^2 - x_4^2.$$

There is an isomorphism given by conjugation between the groups $\mathrm{O}_Q(\mathbb{C})$ and $\mathrm{O}_{\tilde{Q}}(\mathbb{C})$ which maps $\mathrm{O}_Q(\mathbb{Z}[\frac{1}{2}])$ onto $\mathrm{O}_{\tilde{Q}}(\mathbb{Z}[\frac{1}{2}])$. Denote by $A' \subset \mathrm{O}_{\tilde{Q}}(\mathbb{Z}[\frac{1}{2}])$ the image of the Apollonian group $A \subset \mathrm{O}_Q(\mathbb{Z})$ under this isomorphism. Then A' is in fact contained in $\mathrm{O}_{\tilde{Q}}(\mathbb{Z})$.

Proof. Let Q' be the form $Q'(x_1, x_2, x_3, x_4) = -4x_1^2 + 4x_2^2 + 4x_3^2 + 4x_4^2$. It is equivalent to the Descartes form Q, since $Q' = M^T Q M$, where

$$M = \begin{pmatrix} 1 & 0 & -1 & 1 \\ 1 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & -1 & 0 \end{pmatrix}. \tag{2.3}$$

The group $O_{Q'}(\mathbb{Z}[\frac{1}{2}])$ fixing Q' is isomorphic to the group $O_{\tilde{Q}}(\mathbb{Z}[\frac{1}{2}])$, where

$$\tilde{Q}(x_1, x_2, x_3, x_4) = x_1^2 - x_2^2 - x_3^2 - x_4^2. \tag{2.4}$$

Since every element in A is congruent to the identity mod 2, we have that $A \subset \mathrm{O}_Q(\mathbb{Z})$ is mapped to a group $A' \subset \mathrm{O}_{\tilde{Q}}(\mathbb{Z})$ as desired. □

The Apollonian group A is thus isomorphic to a subgroup of $\mathrm{O}_{\tilde{Q}}(\mathbb{Z})$ which we denote by A'. We denote the isomorphism by s:

[4] There is a small typo in the formula printed in [7]. It is corrected here.

$$A' \xrightarrow{s} A \tag{2.5}$$

and relate A' to $\mathrm{SL}_2(\mathbb{Z}(i))$ via the homomorphism ρ in 2.1. Specifically, we get

$$\rho\big(\mathrm{SL}_2\big(\mathbb{Z}(i)\big)\big) = A' \cap \mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$$

where the intersection $A' \cap \mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$ consists of elements of A' with positive determinant. It is known (see [7]) that ρ is in fact a surjection from $\mathrm{SL}_2(\mathbb{Z}(i))$ onto $\mathrm{SO}^+_{\tilde{Q}}(\mathbb{Z})$, a subgroup of index 2 in $\mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$ consisting precisely of matrices of $\mathrm{SO}_{\tilde{Q}}$ with a positive entry in the upper left corner. It is easy to check that every element of $A' \cap \mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$ is in $\mathrm{SO}^+_{\tilde{Q}}$, so we think of ρ as a homomorphism from Γ onto $A' \cap \mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$. Similarly, we have an onto homomorphism from Γ to $A \cap \mathrm{SO}_Q(\mathbb{Z})$ via the isomorphism s:

$$\Gamma \xrightarrow{s\circ\rho} A \cap \mathrm{SO}_Q(\mathbb{Z}),$$

so by considering Γ we simultaneously consider the Apollonian group A as well. The explicit formula for ρ in 2.1 combined with the fact that $A \cap \mathrm{SO}_Q(\mathbb{Z})$ is generated by S_1S_2, S_2S_3, and S_2S_4 and their inverses, where S_i are the generators of A defined in (4.9) allows us to determine exactly the generators and relations of Γ. We describe this in the following lemma.

Lemma 2.3. *Let ρ and A' be as above. The preimage Γ of A' under ρ is a free group generated by $\pm\gamma_1$, $\pm\gamma_2$, $\pm\gamma_3$ and their inverses, where γ_i are as below.*

$$\gamma_1 = \begin{pmatrix} 2 & -i \\ -i & 0 \end{pmatrix}, \qquad \gamma_2 = \begin{pmatrix} -2-2i & -4-3i \\ i & 2i \end{pmatrix}, \qquad \gamma_3 = \begin{pmatrix} 1 & -4i \\ 0 & 1 \end{pmatrix}. \tag{2.6}$$

This follows from applying the homomorphism ρ together with the map s to the generators. Note that this group is a free subgroup of SL_2 – since the elements S_1S_2, S_2S_3, and S_2S_4 have no relations in A, the same holds for the elements $\gamma_i \in \Gamma$. In the next section we use Lemma 2.3 to determine the reduction of Γ mod ideals (d) where d is square-free. We note, however, that to analyze A mod even integers it is not enough to consider the reduction of Γ mod ideals (d) where d is even, since the isomorphism in (2.5) is defined over $\mathbb{Z}(1/2)$. We deal with this separately in Section 4.

2.2. The reduction of Γ mod square-free (d)

Recall from Lemma 1.6 that A is Zariski dense in O_Q, we have $A \cap \mathrm{SO}_Q$ is Zariski dense in SO_Q, and so the group Γ is also Zariski dense in SL_2. We can also check that the subfield of $k = \mathbb{Q}(\sqrt{-1})$ generated by 1 and the traces of the group Γ is in fact the whole field k. For example, the trace of

$$\gamma_1\gamma_2\gamma_3 = \begin{pmatrix} -3-4i & -22+6i \\ 2i-2 & 12i+5 \end{pmatrix} \tag{2.7}$$

is $2+8i$, and the field generated by this trace and 1 is indeed all of k. Thus by Theorem 2.1 we have that outside a finite set of prime ideals $\mathfrak{P} \subset \mathbb{Z}(\sqrt{-1})$ the projection of Γ into $\mathrm{SL}_2/\mathfrak{p}$ is surjective for $\mathfrak{p} \notin \mathfrak{P}$. Our goal is to specify this set $\mathfrak{P}$ and thus determine what the reduction of Γ is mod arbitrary square-free ideals (d). Given the generators of Γ as well as Theorem 2.1, this is a question of elementary group theory. We use a classification due to L.E. Dickson (Theorem 8.27 in [14]) of subgroups of PSL_2 over finite fields:

Theorem 2.4 *(Dickson, 1901). Let q be a power of a prime $p \geqslant 5$. Then the following are the only possible proper subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$.*

(1) *Elementary abelian p-groups*;
(2) *Cyclic groups of order z where* $z \mid \frac{q\pm1}{2}$;
(3) *Dihedral groups of order* $q \pm 1$ *and their subgroups*;
(4) *Semidirect products of elementary abelian groups of order* p^r *and cyclic groups of order t where* $t \mid p^r - 1$ *and* $t \mid q - 1$;
(5) A_4, S_4, *or* A_5;
(6) $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ *where* $p^r \mid q$.

For q prime, the proper subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ given by Theorem 2.4 are metabelian – their commutator subgroups are abelian – except for the groups of small order in (5) (see [5] for a proof). This is also true for proper subgroups of $\mathrm{PSL}_2(\mathbb{F}_{p^2})$ which properly contain $\mathrm{PSL}_2(\mathbb{F}_p)$ for p prime. We use this classification to prove the following proposition regarding the reduction of Γ mod square-free d.

Proposition 2.5. *Let* Γ *and* $\mathcal{O}$ *be as before, let* $\mathfrak{p}$ *denote a prime ideal in* $\mathcal{O}$*, and let* $(d) \neq \mathcal{O}$ *denote an ideal generated by* $d \in \mathcal{O}$*. Let* $\mathfrak{P} = (6)$ *and write* $d = d_1 c$*, where* $(c) \supseteq \mathfrak{P}$ *and* $(d_1) = \prod \mathfrak{p}_i$ *is a product of prime ideals such that* $\mathfrak{p}_i \not\supset \mathfrak{P}$ *for any i. Let* $\Gamma_{\mathfrak{j}}$ *denote the image of* Γ *in* $\mathrm{SL}_2(\mathcal{O}/\mathfrak{j})$ *where* $\mathfrak{j}$ *is an ideal in* $\mathcal{O}$*. Then*:

1) *The projection* $\Gamma_d \longrightarrow \Gamma_c \times \Gamma_{d_1}$ *is surjective.*
2) *The projection* $\Gamma_{d_1} \longrightarrow \prod_{\mathfrak{p}_i \supset (d_1)} \Gamma_{\mathfrak{p}_i}$ *is surjective and* $\Gamma_{\mathfrak{p}_i} = \mathrm{SL}_2(\mathcal{O}/\mathfrak{p}_i)$.

Proof. We first consider the reduction of Γ mod prime ideals $\mathfrak{p} \in \mathcal{O}$ to show that $\Gamma_{\mathfrak{p}}$ is in fact all of SL_2 for $\mathfrak{p} \not\supset \mathfrak{P}$, and then show that Γ maps as a product group as stated in the proposition. We split this up into three cases:

(1) $\mathfrak{p}^2 = (2)$;
(2) $\mathfrak{p}\bar{\mathfrak{p}} = (p)$ where $p \equiv 1 \pmod 4$; here p splits in $\mathcal{O}$, and -1 is a square mod p, so the reduction of Γ mod (p) is mapped to $\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$;
(3) $\mathfrak{p} = (p)$ where $p \equiv 3 \pmod 4$; here p does not split in $\mathcal{O}$, and -1 is not a square mod p, so the reduction of Γ mod (p) is mapped to $\mathrm{SL}_2(\mathbb{F}_{p^2})$.

Case 1. Reducing Γ mod (2) yields a group of order 2, which is clearly not all of $\mathrm{SL}_2(\mathcal{O}/(2))$. Another unpleasant feature of 2 in this context is that it is the only prime which ramifies in $\mathbb{Q}(i)$, since $(2) = (1+i)^2$. We handle the other two cases separately, and note that we will not need to worry about ramification in $\mathbb{Q}(i)$ there.

Case 2. Let $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ where $\bar{\mathfrak{p}}$ is the conjugate of the prime ideal $\mathfrak{p}$ in $\mathcal{O}$. We want to show that Γ reduces onto each factor of $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p}) \times \mathrm{SL}_2(\mathcal{O}/\bar{\mathfrak{p}})$ by first noting that both of these factors are isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$ (we immediately note that the image of Γ in each factor is not trivial – for example, none of the generators of Γ reduce to the identity I mod $\mathfrak{p} \not\supset (2)$). We prove this for $\Gamma_{\mathfrak{p}}$, the reduction of Γ mod $\mathfrak{p}$. The proof in the case of reduction mod $\bar{\mathfrak{p}}$ is then the same argument applied to the conjugate of Γ.

Note that $\Gamma \supset Z(\mathrm{SL}_2)$ contains the center of SL_2 and consider $\Gamma' = \Gamma/Z \subseteq \mathrm{PSL}_2(\mathbb{C})$. If the reduction $\Gamma'_{\mathfrak{p}}$ of Γ' mod $\mathfrak{p}$ is a proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$, it is either metabelian or is one of the groups A_4, S_4, or A_5. We follow [10] to show that this would violate a girth bound for $\Gamma'_{\mathfrak{p}}$ for large enough primes $p = \mathfrak{p}\bar{\mathfrak{p}}$.

Let $S = \{\gamma_1, \gamma_1^{-1}, \gamma_2, \gamma_2^{-1}, \gamma_3, \gamma_3^{-1}\}_{\mathfrak{p}}$ be the set of generators of $\Gamma'_{\mathfrak{p}}$. For example, the generators of $\Gamma'_{(2+i)}$ are

$$\begin{pmatrix} 2 & -2 \\ -2 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

Consider the Cayley graph $C(\Gamma_{\mathfrak{p}}, S)$, where the vertices correspond to elements of $\Gamma_{\mathfrak{p}}$, and two vertices v, w are connected by an edge iff $v = \gamma w$ for some $\gamma \in S$. Define the *girth* $c(\Gamma_{\mathfrak{p}})$ of $C(\Gamma_{\mathfrak{p}}, S)$ to be the length of the shortest cycle in $C(\Gamma_{\mathfrak{p}}, S)$. From [16] we have that

$$c(\Gamma_{\mathfrak{p}}) \geqslant 2\log_{\alpha}(p/2) - 1 \tag{2.8}$$

where

$$\alpha := \max_i \big(\|\gamma_i\|\big).$$

Here we define the norm of a matrix γ as follows:

$$\|\gamma\| := \sup_{\mathbf{x}\neq\mathbf{0}} \frac{\|\gamma\mathbf{x}\|}{\|\mathbf{x}\|}$$

and recall that

$$\|\gamma\|^2 = \big\|\gamma^*\gamma\big\|$$

where γ^* is the conjugate transpose of γ, and the norm of $\gamma^*\gamma$ is its largest eigenvalue. Using this we compute that in our case

$$\alpha = \sqrt{19 + 6\sqrt{10}} = 6.1623\ldots.$$

Thus for $\mathfrak{p}\bar{\mathfrak{p}} = p$ large enough, $\Gamma'_{\mathfrak{p}}$ cannot be A_4, S_4, or A_5 since these groups contain elements of small order which violate the girth bound in (2.8) – for example, these groups contain (12)(34) of order 2. So if $\Gamma'_{\mathfrak{p}}$ is a proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$, it must be metabelian – i.e., for any $A, B, C, D \in \Gamma_{\mathfrak{p}}$ we have

$$\big[[A,B],[C,D]\big] := \big(ABA^{-1}B^{-1}\big)\big(CDC^{-1}D^{-1}\big)\big(BAB^{-1}A^{-1}\big)\big(DCD^{-1}C^{-1}\big) = I. \tag{2.9}$$

However, this yields a cycle of length 16 which also violates the girth bound for primes $p > 2.57\cdot 10^7$, and so $\Gamma'_{\mathfrak{p}} = \mathrm{PSL}_2(\mathbb{F}_p)$ for large enough primes p.

We are left with a finite number of cases which we handle using a program in Matlab. We check that taking $A = \gamma_1$, $B = \gamma_2$, $C = \gamma_3$, and $D = \gamma_1\gamma_2\gamma_3$ where γ_i are as in (2.6) we have

$$\big[[A,B],[C,D]\big] \neq I \tag{2.10}$$

in $\mathrm{PSL}_2(\mathbb{F}_p)$ for $2 < p < 2.57\cdot 10^7$, and thus Γ'_p is not metabelian in these cases. Similarly we check that for $p > 3$ we have $|\Gamma'_{\mathfrak{p}}| > 60$, and so $\Gamma_{\mathfrak{p}} \neq A_4, A_5$, or S_4. Thus $\Gamma'_{\mathfrak{p}} = \mathrm{PSL}_2(\mathbb{F}_p)$ for all primes in this case. Since no proper subgroup of SL_2 maps onto PSL_2 (see [18] for a proof), we have that Γ maps onto $\mathrm{SL}_2(\mathscr{O}/\mathfrak{p})$ and $\mathrm{SL}_2(\mathscr{O}/\bar{\mathfrak{p}})$ as desired.

Case 3. In this case $\mathfrak{p} = (p)$ where $p \equiv 3 \pmod 4$ and we want to show that the reduction $\Gamma_p = \Gamma_{\mathfrak{p}}$ of Γ mod $\mathfrak{p}$ is onto $\mathrm{SL}_2(\mathbb{F}_{p^2})$. Note $\Gamma_p \not\subset \mathrm{SL}_2(\mathbb{F}_p)$ – for example if γ_1/p is the generator γ_1 in Γ_p, we have $\gamma_1/p \notin \mathrm{SL}_2(\mathbb{F}_p)$ for any prime $p \equiv 3 \pmod 4$.

Again, consider $\Gamma' = \Gamma/Z$ as in Case 2. Since Γ'_p properly contains $\mathrm{PSL}_2(\mathbb{F}_p)$, it is a proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_{p^2})$ iff it is one of the groups in parts (1)–(5) of Theorem 2.4 and is thus either metabelian or one of the groups A_4, A_5, or S_4.

The girth bounds calculated in Case 2 again imply that Γ_p' cannot be metabelian for

$$p > 2.57 \cdot 10^7.$$

Similarly, $\Gamma_p' \neq A_4, A_5$, or S_5 for p in this range, and so $\Gamma_p' = \mathrm{PSL}_2(\mathbb{F}_{p^2})$ for large enough p. As in Case 2, we check that if $A = \gamma_1$, $B = \gamma_2$, $C = \gamma_3$, and $D = \gamma_1\gamma_2\gamma_3$,

$$\big[[A, B], [C, D]\big] \neq I$$

in Γ_p for $p \geqslant 3$, and that $|\Gamma_p| > 120$ for $p > 3$. We also check that for $p > 3$ we have $|\Gamma_p| > 120$ and so $|\Gamma_p'| > 60$. Thus Γ maps onto $\mathrm{SL}_2(\mathbb{F}_{p^2})$ for $p > 3$.

If $p = 3$, however, $\Gamma_p' = \mathrm{A}_5$ and so Γ_p is not the full $\mathrm{SL}_2(\mathbb{F}_9)$.

It remains to show that Γ maps as a product group onto the second factor in $\Gamma_c \times \mathrm{SL}_2(\mathscr{O}/(d_1))$. For this we need the following.

Theorem 2.6 *(Goursat's lemma). Let G, G' be groups, and let H be a subgroup of $G \times G'$ such that the two projections $\pi_1 : H \longrightarrow G$ and $\pi_2 : H \longrightarrow G'$ are surjective. Let N be the kernel of π_1, and let N' be the kernel of π_2. Then the image of H in $G/N \times G'/N'$ is the graph of an isomorphism $G/N \cong G'/N'$.*

We have shown above that Γ maps onto $\mathrm{SL}_2(\mathbb{F}_{q^2})$ where $q > 3$ is a prime congruent to 3 mod 4, and onto $\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$ where p is a prime congruent to 1 mod 4. To verify the product structure of $\Gamma/(d_1)$ in Proposition 2.5, we prove the following two lemmas.

Lemma 2.7. *Let Γ, d, c, and d_1 be as in Proposition* 2.5*, let p denote a prime such that $p \equiv 1$ (4), and let $q > 3$ denote a prime such that $q \equiv 3$ (4). Write $d_1 = \prod_{p|d_1} p \prod_{q|d_1} q$, and let*

$$H_q = \mathrm{SL}_2(\mathbb{F}_{q^2}), \qquad G_q = \mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p).$$

Then the projection

$$\Gamma_{(d)} \longrightarrow \Gamma_{(c)} \times \Gamma_{(d_1)}$$

is surjective onto each factor, and the diagonal projection

$$\Gamma_{(d_1)} \longrightarrow \prod_{q|d_1} H_q \times \prod_{p|d_1} G_p \tag{2.11}$$

is surjective onto each factor.

The centers $Z(H_q)$ and $Z(G_p)$ are finite, and the factor groups $H_q/Z(H_q)$ and $G_p/Z(G_p)$ are of the form $\mathrm{PSL}_2(\mathbb{F}_p)$ which is simple for $p > 4$, so its composition factors consist of itself and the trivial group. Therefore H_q and G_p have no composition factors in common for large enough primes p and q, so Theorem 2.6 immediately implies Lemma 2.7. However, since every prime ideal (p) in the product in (2.11) splits, we have that $p = \mathfrak{p}\bar{\mathfrak{p}}$ and we must still show that every G_p maps as a product onto its two factors as in the next lemma.

Lemma 2.8. *Let $\mathscr{O}$ and G_p be as before, where $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ and $\mathfrak{p}$ is a prime ideal in $\mathscr{O}$. Then the diagonal projection*

$$G_p \longrightarrow \mathrm{SL}_2(\mathscr{O}/\mathfrak{p}) \times \mathrm{SL}_2(\mathscr{O}/\bar{\mathfrak{p}}) \tag{2.12}$$

is surjective onto each factor.

Proof. In this case, Theorem 2.6 is not immediately applicable as it was in the proof of Lemma 2.7 since it is not the case that the groups in (2.12) have no composition factors in common. Suppose G_p does not map as a product group onto $\mathrm{SL}_2(\mathscr{O}/\mathfrak{p}) \times \mathrm{SL}_2(\mathscr{O}/\bar{\mathfrak{p}})$. Then by Theorem 2.6 the projection of G_p onto each factor is an isomorphism. In this case, we can write

$$G_p = \big\{\big(x, f(x)\big) \,\big|\, x \in \mathrm{SL}_2(\mathscr{O}/\mathfrak{p})\big\},$$

where f is an isomorphism from $\mathrm{PSL}_2(\mathscr{O}/\mathfrak{p})$ to $\mathrm{SL}_2(\mathscr{O}/\bar{\mathfrak{p}})$. So identifying each of the factors of G_p with the group $H = \mathrm{SL}_2(\mathbb{F}_p)$, every element of G_p is of the form $(x, \phi(x))$, where $x \in H$, and ϕ is an automorphism of H. Since all automorphisms of H are inner, ϕ preserves the trace for every $x \in H$:

$$\mathrm{Tr}\big(\phi(x)\big) = \mathrm{Tr}(x) \quad \text{for all } x \in H.$$

However, we find an element in G_p whose trace is not in $\mathbb{Q}$, and so the element's trace in the first factor is not the same as its trace in the second factor for any $\mathfrak{p}$:

$$\begin{pmatrix} -3-4i & -22+6i \\ 2i-2 & 12i+5 \end{pmatrix}, \tag{2.13}$$

so we have a contradiction, and thus G_p maps as a product onto $\mathrm{SL}_2(\mathscr{O}/\mathfrak{p}) \times \mathrm{SL}_2(\mathscr{O}/\bar{\mathfrak{p}})$ as desired. □

Proposition 2.5 follows from Lemma 2.7, Lemma 2.8, and our case analysis above. □

Proposition 2.5 gives us a concrete description the reduction mod square-free odd integers d of the Apollonian group itself via the spin-homomorphism ρ. It is desirable, however, to understand the structure of A and its orbit under reduction mod any d. To this end we specify the reduction of Γ mod powers of prime ideals $\mathfrak{p}^r$ in the next section.

3. Congruence obstructions: the non-square-free case

In Section 2.2 we proved that Γ has a multiplicative structure under reduction mod square-free ideals (d) outside a finite set of primes. In this section, we extend this multiplicativity to reduction mod *any* (d) by considering the image of Γ mod powers of primes $\mathfrak{p}$. An essential tool in this consideration is a generalization of the following theorem of J.P. Serre (see [18] for a proof).

Theorem 3.1 *(Serre, 1968). Let p be a prime greater than* 3. *If X is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ whose image in $\mathrm{SL}_2(\mathbb{F}_p)$ is $\mathrm{SL}_2(\mathbb{F}_p)$, we have $X = \mathrm{SL}_2(\mathbb{Z}_p)$.*

We extend this theorem to apply in the situation of $\Gamma \subset \mathrm{SL}_2(\mathbb{C})$ below.

Lemma 3.2. *Let $\mathscr{O}$ be the ring of integers in $\mathbb{Q}(i)$ as before. Let $\mathfrak{q} \neq (1+i)$ or* (3) *be a prime ideal in $\mathscr{O}$ and let $\mathscr{O}_\mathfrak{q}$ denote the completion of $\mathscr{O}$ at $\mathfrak{q}$. Let G be a closed subgroup of $\mathrm{SL}_2(\mathscr{O}_\mathfrak{q})$. If the projection of G into $\mathrm{SL}_2(\mathscr{O}_\mathfrak{q}/\mathfrak{q})$ is surjective, then $G = \mathrm{SL}_2(\mathscr{O}_\mathfrak{q})$.*

The proof of this follows the same argument as the proof of Theorem 3.1 in [18] – we outline a modification of it in the special case of reduction mod powers of (2) below. Since the projection of Γ into $\mathrm{SL}_2(\mathscr{O}_\mathfrak{q}/\mathfrak{q})$ is surjective for all but finitely many primes $\mathfrak{q}$ by Proposition 2.5 we may use the result in Lemma 3.2 to determine the reduction of Γ mod powers of $\mathfrak{q}$. We first handle the reduction mod powers of prime ideals $\mathfrak{q}$ contained in the ideals (2) and (3) in the following lemma and obtain the complete picture in Theorem 3.5.

Lemma 3.3. *Let Γ and $\mathscr{O}$ be as before. Let $K_n(2)$ denote the kernel of the projection of $\mathrm{SL}_2(\mathscr{O}/(2^n))$ onto $\mathrm{SL}_2(\mathscr{O}/(2^{n-1}))$, and let $K_n(3)$ denote the kernel of the projection of $\mathrm{SL}_2(\mathscr{O}/(3^n))$ onto $\mathrm{SL}_2(\mathscr{O}/(3^{n-1}))$. Denoting the reduction of Γ mod (d) by Γ_d, we have*

(i) $\Gamma_2 = D_1$, *the dihedral group containing 2 elements.*
(ii) Γ_4 *is an abelian group of 8 elements.*
(iii) *Let τ_n denote the projection of Γ_{2^n} onto $\Gamma_{2^{n-1}}$. The kernel of this projection is $K_n(2)$ for $n \geqslant 4$.*
(iv) $\Gamma_3/Z(\Gamma_3) = \mathsf{A}_5$.
(v) *Let σ_n denote the projection of Γ_{3^n} onto $\Gamma_{3^{n-1}}$. The kernel of this projection is $K_n(3)$ for $n \geqslant 2$.*

Proof. The images of Γ mod (2) and (4) are seen trivially from the generators of Γ, while the image under reduction mod (3) can be deduced from Theorem 2.4.

The number of elements in the kernels of τ_3 and τ_4 can be computed using a simple program in Matlab, and we obtain

$$\begin{aligned} \big|\{\gamma \in \Gamma_{16} \mid \tau_4(\gamma) = I\}\big| &= 520 = \big|K_4(2)\big|, \\ \big|\{\gamma \in \Gamma_9 \mid \sigma_2(\gamma) = I\}\big| &= 738 = \big|K_2(3)\big|. \end{aligned} \tag{3.1}$$

Thus the kernel of τ_4, respectively σ_2, is the full kernel $K_4(2)$, respectively $K_2(3)$. We proceed as in [18] to prove part (iii) of the lemma for $n \geqslant 4$. The proof of part (v) regarding the kernel of σ_n for $n \geqslant 2$ is identical.

Let π_n be the canonical homomorphism from $\mathrm{SL}_2(\mathscr{O}/(2^n))$ onto $\mathrm{SL}_2(\mathscr{O}/(2^{n-1}))$, and let ϕ_n be the projection from $\mathrm{SL}_2(\mathscr{O}/(2^n))$ onto Γ_{2^n}. The following diagram commutes for $n \geqslant 4$:

$$\begin{array}{ccc} \Gamma_{2^{n-1}} & \xleftarrow{\ \tau_n\ } & \Gamma_{2^n} \\ \uparrow{\scriptstyle \phi_n} & & \uparrow{\scriptstyle \phi_n} \\ \mathrm{SL}_2(\mathscr{O}/(2^{n-1})) & \xleftarrow{\ \pi_n\ } & \mathrm{SL}_2(\mathscr{O}/(2^n)) \end{array} \tag{3.2}$$

We want to show that $\ker(\tau_n) = \ker(\pi_n)$ for $n \geqslant 4$. We prove this by induction on n.

From (3.1), this is true in the base case, $n = 4$. We suppose it is true for n, and show that it must also be true for $n+1$. Let X denote the inverse limit of the groups Γ_{2^i} for $i \geqslant 4$:

$$X := \varprojlim \Gamma_{2^i} \quad \text{where } i \geqslant 4$$

and denote by

$$\mathrm{SL}_2(\mathscr{O}_2) := \varprojlim \mathrm{SL}_2(\mathscr{O}/(2^i))$$

the inverse limit of the groups $\mathrm{SL}_2(\mathscr{O}/(2^i))$. We would like to show that for any $\gamma \in \mathrm{SL}_2(\mathscr{O}_2)$ congruent to the identity $\mathscr{I}$ mod 2^n, there is an element $x \in X$ such that

$$x \equiv \gamma \pmod{2^{n+1}}.$$

As in [18], we write

$$\gamma = \mathscr{I} + 2^n \mu.$$

Since $\det(\gamma) = 1$, we must have that $\operatorname{Tr}(\mu) \equiv 0 \pmod 2$. Thus μ can be written mod 2 as a sum of some matrices μ_i such that $\mu_i^2 = 0$, and so $\mu^2 \equiv 0 \pmod 2$.

By the induction hypothesis, we have that there is an element $\beta \in X$ such that

$$\beta = \mathscr{I} + 2^{n-1}\mu + 2^n\delta,$$

where δ has entries in $\mathbb{Z}_2(i)$. Let $x = \beta^2$. That is, we have

$$x = \mathscr{I} + 2^n\mu + 2^{n+1}\delta + 2^{2n-2}\mu^2 + 2^{2n-1}\mu\delta + 2^{2n-1}\delta\mu + 2^{2n}\delta^2.$$

Since $n \geqslant 5$ and $\mu^2 \equiv 0 \bmod 2$, we have produced an element $x \in X$ such that

$$x \equiv \mathscr{I} + 2^n\mu \pmod{2^{n+1}}$$

as desired. □

It remains to determine the image of Γ under reduction mod (c), where $c = 2^n 3^m$. It turns out that powers of (2) do not interact with powers of (3) at all in this context – namely, Γ_c is simply the product of Γ_{2^n} and Γ_{3^n}.

Lemma 3.4. *Let Γ and c be as above. Then*

$$\Gamma_c = \Gamma_{2^n} \times \Gamma_{3^m}.$$

Proof. It is easy to check that the groups Γ_{2^n} and Γ_{3^m} have no composition factors in common for any n and m. The order of Γ_{2^n} is a power of 2, and the same is true of its composition factors. The orders of the composition factors of Γ_{3^n}, however, are all divisible by a power of 3. Thus our claim follows from Theorem 2.6. □

Theorem 3.5. *Let $d = cd'$, where $c = 2^n 3^m$, and $\gcd(d', c) = 1$. Let*

$$d' = \prod_{1 \leqslant i \leqslant r} p_i^{a_i} \prod_{1 \leqslant j \leqslant s} q_j^{b_j}$$

be the prime factorization of d', where $p_i \equiv 1$ mod 4 for all $1 \leqslant i \leqslant r$, and $q_j \equiv 3$ mod 4 for all $1 \leqslant j \leqslant s$. Then Γ maps as a product group onto

$$\Gamma_c \times \prod_{1 \leqslant i \leqslant r} \left(\mathrm{SL}_2\left(\mathbb{Z}/p_i^{a_i}\right) \times \mathrm{SL}_2\left(\mathbb{Z}/p_i^{a_i}\right)\right) \times \prod_{1 \leqslant j \leqslant s} \mathrm{SL}_2\left(\mathscr{O}_{\mathbb{Z}}/q_j^{b_j}\right), \tag{3.3}$$

where Γ_c is the image of Γ under reduction mod c, as described in Lemma 3.4.

This theorem follows from Proposition 2.5, Lemma 3.3, and Lemma 3.4, as well as the discussion in [18]. It describes completely the structure of $A \cap \mathrm{SO}_Q(\mathbb{Z})$ mod any integer d via the homomorphism ρ together with s. In the next section, we use Theorem 3.5 to describe the orbit of A mod square-free integers d.

4. Congruence obstructions for the orbit

Since we are ultimately interested in the local structure of the orbit of A, we extend Theorem 3.5 to the setting of the orbit $\mathscr{P} = \mathscr{P}(P) = A\mathbf{v}$ where $\mathbf{v} = \mathbf{v}_P$ is a Descartes quadruple of curvatures in a packing P. Throughout this section, we consider the cone

$$C = \left\{\mathbf{v} = (v_1, v_2, v_3, v_4) \;\middle|\; \mathbf{v} \neq \mathbf{0},\ Q(\mathbf{v}) = 0\right\} \tag{4.1}$$

where Q is the Descartes quadratic form. Note that the Apollonian group A acts on C by mapping any quadruple of mutually tangent circles represented by a point of C to another quadruple of mutually tangent circles in the same packing. In other words, for $\alpha \in A$ we have

$$(a, b, c, d) \xrightarrow{\alpha} \left(a', b', c', d'\right)$$

where (a, b, c, d) and (a', b', c', d') are Descartes quadruples in a packing P. We would like to elaborate on how this action behaves under reduction mod integers $d > 1$. Given the multiplicative property of the group Γ in Section 3, this amounts to specifying how orbits of A mod powers of primes sit inside C_{p^r}, defined recursively as follows:

- For $p > 2$,

$$\begin{aligned} C_p &= \left\{\mathbf{v} \in \mathbb{Z}/p\mathbb{Z} \;\middle|\; \mathbf{v} \not\equiv \mathbf{0}\ (p),\ Q(\mathbf{v}) \equiv 0\ (p)\right\}, \\ C_{p^r} &= \left\{\mathbf{v} \in \mathbb{Z}/p^r\mathbb{Z} \;\middle|\; \mathbf{v} \in C_{p^{r-1}}\left(p^{r-1}\right),\ Q(\mathbf{v}) \equiv 0\left(p^r\right)\right\} \end{aligned} \tag{4.2}$$

  for $r > 1$.
- For $p = 2$,

$$\begin{aligned} C_2 &= \left\{\mathbf{v} \in \mathbb{Z}/2\mathbb{Z} \;\middle|\; \mathbf{v} \not\equiv \mathbf{0}\ (2),\ Q(\mathbf{v}) \equiv 0\ (2)\right\}, \\ C_{2^r} &= \left\{\mathbf{v} \in \mathbb{Z}/2^r\mathbb{Z} \;\middle|\; \mathbf{v} \in C_{2^{r-1}}\left(2^{r-1}\right),\ Q(\mathbf{v}) \equiv 0\left(2^r\right),\ \exists \mathbf{w} \equiv \mathbf{v}\left(2^r\right) \text{ s.t. } Q(\mathbf{w}) \equiv 0\left(2^{r+1}\right)\right\} \end{aligned} \tag{4.3}$$

  for $r > 1$.

Note that we need to define C_{2^r} separately because it is not true in this case that every solution to $Q(\mathbf{v}) \equiv \mathbf{0}\ (2^r)$ lifts to some solution of the equation mod 2^{r+1} – only half of the solutions mod 2^r lift to solutions mod higher powers, and every element of C_{2^r} as defined above has 8 elements lying above it in $C_{2^{r+1}}$. Furthermore, since the isomorphism in (2.5) is over $\mathbb{Z}[1/2]$, we cannot apply results about Γ to reduction of the orbit mod powers of 2 or mod even integers. We thus consider the reduction of A mod odd integers first, and complete the picture with an analysis of reduction mod powers of 2 in Lemmas 4.3 and 4.4.

Recall that A acts on C by mapping any quadruple of mutually tangent circles represented by a point of C to another quadruple of mutually tangent circles in the same packing. Similarly, the group Γ acts on the cone C via the spin homomorphism ρ and the change of variables map s in (2.5). Namely, for any $\gamma \in \Gamma$, we have the action

$$(a, b, c, d) \xrightarrow{s(\rho(\gamma))} \left(a', b', c', d'\right) \tag{4.4}$$

of γ on a quadruple (a, b, c, d) in the packing P. Since $s(\rho(\gamma)) \in A \cap \mathrm{SO}_Q(\mathbb{Z})$, this action does not depict the whole action of the Apollonian group, but rather only the action of elements of even word length in the four generators of A. However, we can easily relate it to the action of all of A by multiplying on the left by the generator S_1.

Lemma 4.1. *Let $\tilde{A} = A \cap \mathrm{SO}_Q(\mathbb{Z})$, and let $S_1 \in A$ be as in* (4.9)*. Then*

$$A = \tilde{A} \cup S_1 \tilde{A}. \tag{1}$$

In general, we have

$$\mathrm{O}_Q(\mathbb{Z}) = \mathrm{SO}_Q(\mathbb{Z}) \cup S_1 \mathrm{SO}_Q(\mathbb{Z}). \tag{2}$$

Proof. To prove (1), consider $\alpha \in A$, and let $w(\alpha)$ denote the shortest word length of α in the generators S_i of A. Since $\tilde{A} = A \cap \mathrm{SO}_Q(\mathbb{Z})$ and $\det(S_1) = -1$, if $w(\alpha)$ is even then $\alpha \in \tilde{A}$ and we are done. Otherwise, $w(S_1\alpha)$ is even and so $S_1\alpha \in \tilde{A}$. Since $S_1^2 = I$, we have $\alpha \in S_1\tilde{A}$.

Furthermore, note that $S_1 \mathrm{SO}_Q(\mathbb{Z})$ is a coset not containing I, and so $\mathrm{SO}_Q(\mathbb{Z}) \cup S_1 \mathrm{SO}_Q(\mathbb{Z})$ is simply a left coset partition of $\mathrm{O}_Q(\mathbb{Z})$ since $[\mathrm{O}_Q : \mathrm{SO}_Q] = 2$. This proves (2). □

Since we can view the action of the Apollonian group on the cone as the action of Γ in this way, we apply Theorem 3.5 to obtain the desired structure of the orbit of A mod odd integers d in the following lemma.

Lemma 4.2. *Let C and C_{p^r} be as above, let $\mathscr{P}$ be an orbit of A acting on a Descartes quadruple of curvatures $\mathbf{v} = \mathbf{v}_P$ of a packing P and let $\mathscr{P}_d$ be the reduction of this orbit mod an odd integer $d > 1$. Write $d = d_1 d_2$ with $(d_2, 3) = 1$ and $d_1 = 3^m$ where $m \geqslant 0$ is an integer. Then*:

(i) *If $m \geqslant 1$, the natural projection $\mathscr{P}_d \longrightarrow \mathscr{P}_{d_1} \times \mathscr{P}_{d_2}$ is surjective.*
(ii) *If $m \geqslant 1$, let $\pi : C_{d_1} \longrightarrow C_3$ be the natural projection. Then $\mathscr{P}_{d_1} = \pi^{-1}(\mathscr{P}_3)$.*
(iii) *The natural projection $\mathscr{P}_{d_2} \longrightarrow \prod_{p^r \| d_2} \mathscr{P}_{p^r}$ is surjective and $\mathscr{P}_{p^r} = C_{p^r}$.*

Proof. We derive (i) directly from Lemma 4.4 and the product group structure of Γ in Theorem 3.5. This structure translates to the orbit setting via the action in (4.4) of Γ_d on the cone. For simplicity, we refer to this action as $\rho(\gamma)$ as opposed to $s(\rho(\gamma))$ above. Using the notation of (3.3) and assuming $d_1 > 1$, for $\mathbf{v} = \mathbf{v}_P$ we have

$$\begin{aligned}
\rho(\Gamma_d)(\mathbf{v}) &= \rho\Bigg(\Gamma_{d_1} \times \prod_{1 \leqslant i \leqslant r} \mathrm{SL}_2\big(\mathbb{Z}/p_i^{a_i}\big) \times \mathrm{SL}_2\big(\mathbb{Z}/p_i^{a_i}\big) \times \prod_{1 \leqslant j \leqslant s} \mathrm{SL}_2\big(\mathscr{O}/q_j^{b_j}\big)\Bigg)(\mathbf{v}) \\
&= \rho(\Gamma_{d_1})(\mathbf{v}) \times \prod_{1 \leqslant i \leqslant r} \rho\big(\mathrm{SL}_2\big(\mathbb{Z}/p_i^{a_i}\big)\big)(\mathbf{v}) \times \prod_{1 \leqslant j \leqslant s} \rho\big(\mathrm{SL}_2\big(\mathscr{O}/q_j^{b_j}\big)\big)(\mathbf{v}) \\
&= \rho(\Gamma_{d_1})(\mathbf{v}) \times \prod_{p^r \| d_2} \mathrm{SO}_Q\big(\mathbb{Z}/\big(p^r\mathbb{Z}\big)\big)(\mathbf{v}).
\end{aligned} \tag{4.5}$$

Combining this with the multiplication of S_1 by $\rho(\Gamma_d)(\mathbf{v})$ in Lemma 4.1 we get

$$\begin{aligned}
\mathscr{P}_d &= S_1 \cdot \rho(\Gamma_d)(\mathbf{v}) \cup \rho(\Gamma_d)(\mathbf{v}) = \big(S_1 \cdot \rho(\Gamma_{d_1})(\mathbf{v}) \cup \rho(\Gamma_{d_1})(\mathbf{v})\big) \times \prod_{p^r \| d_2} C_{p^r} \\
&= \mathscr{P}_{d_1} \times \prod_{p^r \| d_2} C_{p^r}
\end{aligned}$$

as desired.

We prove (ii) in a similar way, using the characterization of Γ_c in Lemma 3.4. To realize the structure of $\rho(\Gamma_{3^m})(\mathbf{v})$, note that the following diagram, where τ_m and τ'_m are the natural projections obtained by reduction mod 3^m, is commutative:

$$\begin{array}{ccc} \tilde{A}_{3^m} & \xleftarrow{\tau'_m} & \tilde{A}_{3^{m+1}} \\ \rho \uparrow & & \rho \uparrow \\ \Gamma_{3^m} & \xleftarrow{\tau_m} & \Gamma_{3^{m+1}} \end{array} \tag{4.6}$$

We recall from Lemma 3.4 that $\ker(\tau_m) = K_m(3)$ for $m \geqslant 2$, where $K_m(3)$ is the kernel of the projection

$$\mathrm{SL}_2(\mathscr{O}/3^{m+1}) \xrightarrow{\pi_n} \mathrm{SL}_2(\mathscr{O}/3^m)$$

and therefore

$$\ker\bigl(\tau'_m\bigr) = \rho\bigl(\ker\bigl(\tau(m)\bigr)\bigr) = \rho\bigl(K_m(3)\bigr).$$

Let π'_m be the projection from $\mathrm{SO}_Q(\mathbb{Z}/3^m\mathbb{Z})$ onto $\mathrm{SO}_Q(\mathbb{Z}/3^{m-1}\mathbb{Z})$, and let $K'_m(3)$ be the kernel of π'_m. Since the diagram

$$\begin{array}{ccc} \mathrm{SO}_Q(\mathbb{Z}/3^m\mathbb{Z}) & \xleftarrow{\pi'_m} & \mathrm{SO}_Q(\mathbb{Z}/3^{m-1}\mathbb{Z}) \\ \rho \uparrow & & \rho \uparrow \\ \mathrm{SL}_2(\mathscr{O}/3^m) & \xleftarrow{\pi_m} & \mathrm{SL}_2(\mathscr{O}/3^{m-1}) \end{array} \tag{4.7}$$

also commutes, we have that $\rho(K_m(3)) = K'_m(3)$ for $m \geqslant 2$. Finally, we note that the diagram

$$\begin{array}{ccc} C_{3^m} & \longleftarrow & C_{3^{m+1}} \\ \uparrow & & \uparrow \\ \mathscr{P}_{3^m} & \longleftarrow & \mathscr{P}_{3^{m+1}} \end{array} \tag{4.8}$$

commutes for $m \geqslant 2$. Combined with our analysis of the kernel of τ'_m above, we have that every $\mathbf{v} \in C_{3^{m+1}}$ lying above a vector $\mathbf{v} \in \mathscr{P}_{3^m}$ is also in $\mathscr{P}_{3^{m+1}}$. Thus $\mathscr{P}_{3^m} = \pi^{-1}(\mathscr{P}_3)$ as desired. □

It remains to extend Lemma 4.2 to all integers d. We first prove an analog of part (ii) of Lemma 4.2 for powers of 2.

Lemma 4.3. *Let $\mathscr{P}$ be a primitive integer orbit of the Apollonian group, and let $\mathscr{P}_{2^n}$ denote the reduction of $\mathscr{P}$ mod 2^n. Let C_{2^n} be as in* (4.3) *and let π_n be the natural projection*

$$\pi_n : C_{2^n} \longrightarrow C_{2^{n-1}}.$$

With this notation, we have

$$\mathscr{P}_{2^n} = \pi_n^{-1}(\mathscr{P}_{2^{n-1}})$$

for $n \geqslant 4$. In particular, if $\pi : C_{2^n} \longrightarrow C_8$ is the natural projection where $n \geqslant 4$, then $\mathscr{P}_{2^n} = \pi^{-1}(\mathscr{P}_8)$.

Proof. To prove this, we produce elements of A which effectively lift points in $\mathscr{P}_{2^{n-1}}$ to all possible points in C_{2^n}. Let S_1, S_2, S_3, and S_4 be the generators of the Apollonian group as before, and let $X_0 = S_2S_1S_3$, $Y_0 = S_1S_2S_4$, $Z_0 = S_1S_3$. For integers $n \geqslant 4$, let $X(n) = X_0^{2^{n-3}}$, $Y(n) = Y_0^{2^{n-3}}$, and $Z(n) = Z_0^{2^{n-3}}$. We have

$$
\begin{aligned}
X(n) &\equiv \begin{pmatrix} 1 & 2^{n-1} & 2^{n-1} & 0 \\ 2^{n-1} & 1 & 2^{n-1} & 0 \\ 2^{n-1} & 2^{n-1} & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \pmod{2^n}, \\
Y(n) &\equiv \begin{pmatrix} 1 & 2^{n-1} & 0 & 2^{n-1} \\ 2^{n-1} & 1 & 0 & 2^{n-1} \\ 0 & 0 & 1 & 0 \\ 2^{n-1} & 2^{n-1} & 0 & 1 \end{pmatrix} \pmod{2^n}, \\
Z(n) &\equiv \begin{pmatrix} 2^{n-2}+1 & 2^{n-2} & -2^{n-2} & 2^{n-2} \\ 0 & 1 & 0 & 0 \\ 2^{n-2} & -2^{n-2} & 1-2^{n-2} & -2^{n-2} \\ 0 & 0 & 0 & 1 \end{pmatrix} \pmod{2^n}. \qquad (4.9)
\end{aligned}
$$

Let H_n be the abelian group of order 16 generated by $X(n)$, $Y(n)$, and $Z(n)$ mod 2^n. Note that any primitive orbit $\mathscr{P}$ of A mod 2 consists of one vector, where two coordinates are 1's, and two coordinates are 0's (this follows from the unique nontrivial solution to the Descartes equation mod 2), and that we can arrange the vector to be $(1,0,0,1)$ and re-order coordinates of all the vectors in the orbit accordingly. With this in mind, let $n \geqslant 4$, and let $\mathbf{r} \in \mathscr{P}$ be the vector

$$\mathbf{r} = \left(a + 2^{n-1}k_1, b + 2^{n-1}k_2, c + 2^{n-1}k_3, d + 2^{n-1}k_4\right)^T$$

which is $(a,b,c,d)^T$ mod 2^{n-1}. Here $0 \leqslant a,b,c,d < 2^{n-1}$ are integers such that a and d are odd and b and c are even. Since H_n is a subgroup of A, we have that the orbit $H_n\mathbf{r}$ mod 2^n sits inside $\mathscr{P}_{2^n}$. In particular, given that

- $\mathbf{v} \equiv (1,0,0,1)^T \pmod 2$,
- $v_1 + v_2 + v_3 + v_4 \equiv 0 \pmod 2$,
- $v_1 + v_2 + v_3 + v_4 \equiv 0 \pmod 4$

for every $\mathbf{v} = (v_1, v_2, v_3, v_4)^T \in \mathscr{P}$, we have

$$
\begin{aligned}
\mathscr{I} \cdot \mathbf{r} &\equiv \mathbf{r}, \\
Y(n) \cdot \mathbf{r} &\equiv \mathbf{r} + \left(2^{n-1}, 0, 0, 2^{n-1}\right)^T, \\
Z(n) \cdot \mathbf{r} &\equiv \mathbf{r} + \left(2^{n-1}, 0, 0, 0\right)^T, \\
X(n)Z(n) \cdot \mathbf{r} &\equiv \mathbf{r} + \left(2^{n-1}, 2^{n-1}, 2^{n-1}, 0\right)^T, \\
Y(n)Z(n) \cdot \mathbf{r} &\equiv \mathbf{r} + \left(0, 0, 0, 2^{n-1}\right)^T, \\
X(n)Y(n)Z(n) \cdot \mathbf{r} &\equiv \mathbf{r} + \left(0, 2^{n-1}, 2^{n-1}, 2^{n-1}\right)^T, \\
X(n) \cdot \mathbf{r} &\equiv \mathbf{r} + \left(0, 2^{n-1}, 2^{n-1}, 0\right)^T, \\
X(n)Y(n) \cdot \mathbf{r} &\equiv \mathbf{r} + \left(2^{n-1}, 2^{n-1}, 2^{n-1}, 2^{n-1}\right)^T
\end{aligned}
$$

mod 2^n. This is the full list of points in C_{2^n} lying above $\mathbf{r}$, as desired. □

Finally, we show a multiplicative structure for orbits of the Apollonian group mod even integers in the following lemma:

Lemma 4.4. *Let $\delta = 2^n$ be any positive power of 2 and let $\mathscr{P}$ be as before. Let c be an odd integer, and let $d = \delta c$. Then the projection*

$$\mathscr{P}_d \longrightarrow \mathscr{P}_\delta \times \mathscr{P}_c$$

is surjective.

Proof. Let $c = 3^m c'$, where $\gcd(c', 3) = 1$ and $m \geqslant 0$. For $\tilde{A} = A \cap \mathrm{SO}_Q$, let $\tilde{A}_d$ denote the reduction of $\tilde{A}$ mod d. From the proof of Lemma 4.2, we have that $\tilde{A}_c$ maps as a product group onto

$$\tilde{A}_{3^m} \times \prod_{p^r \| c'} \mathrm{SO}_Q\left(\mathbb{Z}/p^r\mathbb{Z}\right) \tag{4.10}$$

if $m \geqslant 1$, or as a product group onto the second factor in (4.10). Assume $m \geqslant 1$, and note that the projection $\tilde{A}_d$ to

$$\tilde{A}_\delta \times \tilde{A}_{3^m} \times \prod_{p^r \| c'} \mathrm{SO}_Q\left(\mathbb{Z}/p^r\mathbb{Z}\right) \tag{4.11}$$

is onto each factor by the proof of Lemma 4.2. By Goursat's Theorem 2.6, note that the groups in (4.10) have no composition factors in common. Furthermore, the order of $\tilde{A}_\delta$ is a power of 2, and so all of its composition factors also have order a power of 2. However, this is not true of any of the composition factors of $\tilde{A}_{3^m}$ or $\mathrm{SO}_Q(\mathbb{Z}/p^r\mathbb{Z})$, so by Goursat's lemma we have that $\tilde{A}_d$ does indeed map as a product group onto the expression in (4.11). As in Lemma 4.2, we consider the orbit

$$\tilde{A}_d\mathbf{v} = \tilde{A}_\delta \times \tilde{A}_{3^m} \times \prod_{p^r | c'} \mathrm{SO}_Q\left(\mathbb{Z}/\left(p^r\mathbb{Z}\right)\right)(\mathbf{v}) \tag{4.12}$$

and combine this with the multiplication of S_1 as described in Lemma 4.1 to get

$$\begin{aligned}\mathscr{P}_d &= (S_1 \cdot \tilde{A}_d)(\mathbf{v}) \cup \tilde{A}_d\mathbf{v} = A_\delta\mathbf{v} \times \mathscr{P}_{3^m} \times \prod_{p^r | c'} C_{p^r} \\ &= \mathscr{P}_\delta \times \mathscr{P}_c\end{aligned}$$

as desired. The proof in the case of $m = 0$ is identical (the factor of $\mathscr{P}_{3^m}$ is simply omitted). □

Theorem 1.4 follows directly from Lemmas 4.2, 4.3, and 4.4. It implies the following improvement of Graham et al.'s Theorem 1.3.

Corollary 4.5. *Let P be a primitive integral Apollonian circle packing, and let $d > 1$ be a square-free integer such that $\gcd(d, 6) = 1$. The curvatures of circles in P cover all possible congruence classes modulo d.*

Proof. We wish to show that for any residue class k modulo d, k is a coordinate of some vector $\mathbf{v} \in \mathscr{P}$. Suppose $k \neq 0$. Let $C_d = \prod_{p \| d} C_p$. Note that $Q(0, 0, k, k) = 0$ for any $k \neq 0$ where Q is the Descartes form, and so $(0, 0, k, k) \in C_d$ for all $d \in \mathbb{N}$. Since $\mathscr{P}_d = C_d$ for d relatively prime to 6 by Theorem 1.4, we have that $(0, 0, k, k) \in \mathscr{P}_d$ as well, and so we have what we want. If $k = 0$, then we easily produce a vector with coordinate 0 in $\mathscr{P}_d$ – again, $(0, 0, a, a) \in \mathscr{P}_d$ for any $a \neq 0$. □

Note that the corollary above implies that the bad primes (in the sense of Weisfeiler's theorem) for the Apollonian group are 2 and 3. Removing either of these from the set of bad primes is impossible – the corollary does not hold if 6 is replaced by either 2 or 3.

This corollary, combined with Theorem 1.4, completes the local description of curvatures in any given primitive ACP. The next step is to prove a local to global principle as in Conjecture 1.5, and try to understand for which thin groups one might expect such a principle to hold. In addition, it would be interesting to explain how the set of bad primes depends on the group itself. Here, we extract the bad primes via a rather technical process, and being able to avoid this process would be useful in applications of the affine sieve and beyond.

Acknowledgments

We thank Alireza Salehi-Golsefidy and Peter Sarnak for insightful comments and conversations, Alex Kontorovich for the pictures of ACP's in Figs. 2 and 3, and the referee for helpful comments which led to various improvements of this paper.

References

[1] J. Bourgain, E. Fuchs, A proof of the positive density conjecture for integer Apollonian circle packings, J. Amer. Math. Soc. 24 (2011) 945–967.
[2] J. Bourgain, A. Gamburd, P. Sarnak, Affine linear sieve, expanders, and sum-product, Invent. Math. 179 (3) (2010) 559–644.
[3] J. Cogdell, On sums of three squares, J. Thèor. Nombres Bordeaux 15 (2003).
[4] H.S.M. Coxeter, An absolute property of four mutually tangent circles, in: A. Prékopa, E. Molnàr (Eds.), Non-Euclidean Geometries, Jaános Bolyai Memorial Volume, Kluwer Academic Publ., 2005.
[5] G. Davidoff, P. Sarnak, A. Valette, Elementary Number Theory, Group Theory, and Ramanujan Graphs, Cambridge University Press, Cambridge, UK, 2003.
[6] W. Duke, R. Schulze-Pillot, Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids, Invent. Math. 99 (1990) 49–57.
[7] J. Elstrodt, F. Grunewald, J. Mennicke, Groups Acting on Hyperbolic Space, Springer-Verlag, Berlin, Heidelberg, 1998.
[8] E. Fuchs, Arithmetic properties of Apollonian circle packings, PhD thesis, Princeton University, 2010.
[9] E. Fuchs, K. Sanden, Some experiments with integral Apollonian circle packings, Experiment. Math., in press. Preprint is currently available at http://www.math.ias.edu/~efuchs/appoloexperiment.pdf.
[10] A. Gamburd, On the spectral gap for infinite index "congruence" subgroups of $SL_2(\mathbb{Z})$, Israel J. Math. 127 (2002) 157–200.
[11] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.H. Yan, Apollonian circle packings: number theory, J. Number Theory 100 (2003) 1–45.
[12] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.H. Yan, Apollonian circle packings: geometry and group theory. I. The Apollonian group, Discrete Comput. Geom. 34 (2005) 547–585, doi:10.1007/s00454-005-1196-9.
[13] K.E. Hirst, The Apollonian packing of circles, Proc. Natl. Acad. Sci. USA 29 (1943) 378–384.
[14] B. Huppert, Endliche Gruppe I, Springer-Verlag, Berlin, Heidelberg, 1967.
[15] A. Kontorovich, H. Oh, Apollonian circle packings and closed horospheres on hyperbolic 3-manifolds, J. Amer. Math. Soc. 24 (2011) 603–648.
[16] G. Margulis, Explicit construction of graphs without short cycles and low density codes, Combinatorica 2 (1982) 71–78.
[17] C.T. McMullen, Hausdorff dimension and conformal dynamics. III. Computation of dimension, Amer. J. Math. 120 (4) (1998).
[18] J.-P. Serre, Abelian l-Adic Representations and Elliptic Curves, Addison–Wesley Publishing Company, Inc., The Advanced Book Program, New York, 1989.
[19] F. Soddy, The kiss precise, Nature 137 (1937) 1021.
[20] B. Weisfeiler, Strong approximation for Zariski dense subgroups of semi-simple algebraic groups, Ann. of Math. 120 (2) (1984) 271–315.